IMAGE DATA CIPHERING METHOD

Patent Number: JP6125553
Publication date: 1994-05-06
Inventor(s): NAKAI TOSHIHISA
Applicant(s): OKI ELECTRIC IND CO LTD
Requested Patent: JP6125553
Application Number: JP19920273138 19921012
Priority Number (s):
IPC Classification: H04N7/167; G06F15/66; G09C5/00; H04L9/06; H04L9/14; H04N1/41; H04N1/415; H04N1/44; H04N7/133
EC Classification:
Equivalents:

Abstract

PURPOSE:To reduce the processing amount for ciphering.
CONSTITUTION:Inputted image signals are divided into blocks by a blocking part 102, a DCT conversion is performed for the divided blocks by a DCT part 103, and DC components f (0, 0) and AC components f (i, j) are outputted. The DC components f (0, 0) are quantized by a DC quantizing part 104, are ciphered a ciphering part 110 and are delivered to a multiplexing part 131. The AC components f (i, j) is quantized by an AC quantizing part 105 and is delivered to the multiplexing part 131 after an entropy encoding is performed for the components by an AC entropy encoding part 120. In the multiplexing part 131, the output of the ciphering part 110 and the output of the AC entropy encoding part 120 is multiplexed and outputted. Thus, the only DC components of image data are ciphered.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－125553

(43)公開日　平成6年(1994)5月6日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｎ　7/167		8943－5C		
Ｇ０６Ｆ　15/66	３３０　Ｈ	8420－5L		
Ｇ０９Ｃ　5/00		8837－5L		
Ｈ０４Ｌ　9/06				
		7117－5K	Ｈ０４Ｌ　9/02	Ｚ

審査請求　未請求　請求項の数３(全 17 頁)　最終頁に続く

(21)出願番号　特願平4－273138

(22)出願日　平成４年(1992)10月12日

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号

(72)発明者　中井　敏久
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

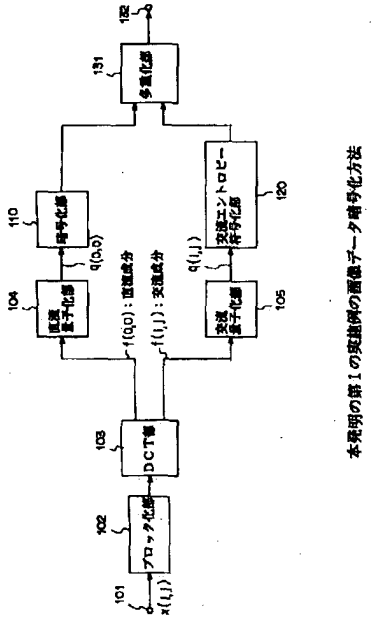
(74)代理人　弁理士　柿本　恭成

(54)【発明の名称】　画像データ暗号化方法

(57)【要約】

【目的】　暗号化のための処理量を少なくする。

【構成】　入力された画像信号がブロック化部１０２でブロックに分割され、その分割されたブロックがＤＣＴ部１０３でＤＣＴ変換され、直流成分ｆ（０，０）と交流成分ｆ（ｉ，ｊ）が出力される。直流成分ｆ（０，０）は、直流量子化部１０４で量子化され、暗号化部１１０で暗号化されて多重化部１３１へ送られる。交流成分ｆ（ｉ，ｊ）は、交流量子化部１０５で量子化され、交流エントロピー符号化部１２０でエントロピー符号化された後、多重化部１３１へ送られる。多重化部１３１では、暗号化部１１０の出力及び交流エントロピー符号化部１２０の出力を多重化して出力する。これにより、画像データのうちの直流成分だけが暗号化される。



本発明の第１の実施例の画像データ暗号化方法

1

【特許請求の範囲】

【請求項1】　圧縮した画像データを暗号化する画像データ暗号化方法において、

2次元の画像信号をｎ画素ｘｎ画素のブロックに分割する分割処理と、

前記分割処理で分割されたブロックを離散コサイン変換する離散コサイン変換処理と、

前記離散コサイン変換処理の出力のうちの直流成分を量子化する直流量子化処理と、

前記離散コサイン変換処理の出力のうちの交流成分を量子化する交流量子化処理と、

前記直流量子化処理の出力を暗号化する暗号化処理と、

前記交流量子化処理の出力をエントロピー符号化する交流エントロピー符号化処理と、

前記暗号化処理の出力と前記交流エントロピー符号化処理の出力とを多重化する多重化処理とを、

実行することを特徴とする画像データ暗号化方法。

【請求項2】　前記直流量子化処理では、出力信号をｎビットの固定長符号に符号化する固定長符号化処理を行い、

前記暗号化処理では、前記直流量子化処理の出力に対してｎビット毎に暗号化し、

前記多重化処理では、１ブロック毎に前記暗号化処理の出力と前記交流エントロピー符号化処理の出力を多重化することを特徴とする請求項１記載の画像データ暗号化方法。

【請求項3】　圧縮した画像データを暗号化する画像データ暗号化方法において、

2次元の画像信号をｎ画素ｘｎ画素のブロックに分割する分割処理と、

前記分割処理で分割されたブロックを離散コサイン変換する離散コサイン変換処理と、

前記離散コサイン変換処理の出力のうちの直流成分を差動符号化する差動符号化処理と、

前記差動符号化処理の出力を量子化する直流量子化処理と、

前記直流量子化処理の出力をエントロピー符号化する直流エントロピー符号化処理と、

前記直流エントロピー符号化処理の出力を暗号化する暗号化処理と、

前記離散コサイン変換処理の出力のうちの交流成分を量子化する交流量子化処理と、

前記交流量子化処理の出力をエントロピー符号化する交流エントロピー符号化処理と、

１画面分の前記暗号化処理の出力ビット数をカウントし、そのカウント値と１画面分の前記暗号化処理の出力と１画面分の前記交流エントロピー符号化処理の出力とを多重化する多重化処理とを、

実行すること特徴とする画像データ暗号化方法。

【発明の詳細な説明】

2

【０００１】

【産業上の利用分野】本発明は、ディジタル化した画像データを暗号化する画像データ暗号化方法に関するものである。

【０００２】

【従来の技術】従来、このような分野の技術としては、例えば次のような文献に記載されるものがあった。

文献１；Communications of the ACM、３４［４］（１９９１－４）（米）Gregory K. Wallace著“ザ　ジェピィイージィ　スティル　ピクチャーコンプレッション　スタンダード（The JPEG Still Picture Compression Standard）”Ｐ．３０－４４

文献２；APPENDIX A.FIPS PUBLICATION46（１９７７－１）U.S.Departmentof Commerce/National Bureau of Standards　発行（米）“データエンクリプション　スタンダード（Date Encrption Standard)”Ｐ．６５３－６７０

文献３；池野・小山著「現代暗号理論」２版（昭６２－６－１０）電子情報通信学会、Ｐ．４３－４９

ここで、文献１は画像データの圧縮方法に関する技術であり、文献２，３はデータの暗号化に関する技術である。

【０００３】図２は、前記文献１に記載された従来の画像データ圧縮方法の一構成例を示すブロック図である。この画像データ圧縮方法では、例えば縦横８画素のブロック画像データDA_iがエンコーダ１０内の離散コサイン変換部（以下、ＤＣＴ部という）１１で離散コサイン変換（以下、ＤＣＴ変換という）され、その変換結果が量子化部１２へ送られる。量子化部１２では、量子化テーブル１４のデータに基づいてＤＣＴ変換の各係数を量子化し、エントロピー符号化部１３へ送る。エントロピー符号化部１３は、符号化テーブル１５のデータに基づき、量子化部１２の出力データに対してエントロピー符号化を行い、圧縮画像データDA_Oを出力する。これにより、縦横８画素のブロック画像データDA_iのデータ圧縮が行える。図３は、前記文献２，３に記載された従来のデータ暗号化方法の一構成例を示すブロック図である。このデータ暗号化方法は、暗号化処理部２０と鍵の生成部３０とでデータの暗号化を行うもので、６４ビットからなる平文レジスタ２１に入力されたデータは、６４ビットからなる鍵レジスタ３１に格納したデータに依存して、図３に示される転置、シフト、排他的論理和等の一連の処理によって暗号化され、６４ビットからなる暗号文レジスタ２３へ出力される。

【０００４】暗号化処理部２０における暗号化処理では、まず６４ビットの平文レジスタ２１に対して初期転置ＩＰの処理が行われる。この初期転置ＩＰの処理の出力に対し、１６段の暗号化処理２２－１～２２－１６が行われる。初段の暗号化処理２２－１では、初期転置ＩＰが行われた６４ビットのデータが、３２ビットずつ左

右に分割され、左半分がL_0、及び右半分がR_0となる。このL_0とR_0からL_{16}とR_{16}になるまで、１６段にわたって暗号化処理２２－１～２２－１６が行われる。その後、初期転置ＩＰと逆の変換を行う最終転置IP^{-1}の処理が行われ、暗号化されたデータが６４ビットの暗号文レジスタ２２に格納される。鍵の生成部３０では、第１段～第１６段の暗号化処理２２－１～２２－１６に必要な１６個の４８ビットの鍵K_1～K_{16}を生成する。まず、パリティビットを含む６４ビットの入力鍵が鍵レジスタ３１に格納される。鍵レジスタ３１の入力鍵に対し、鍵の縮約型転置ＰＣ－１により、転置が行われると共にパリティビットが除かれた５６ビットの鍵となる。この５６ビットの鍵は、２つに分割され、一方の２８ビットがC_0、他方の２８ビットがD_0となる。このC_0とD_0をそれぞれ左に順にシフトすることにより、C_1，D_1からC_{16}，D_{16}が順次生成される。ｎ段目の鍵K_nは、C_nとD_nからなる５６ビットを入力し、鍵の縮約型転置ＰＣ－２を行って４８ビットとなり、第ｎ段の暗号化処理２２－ｎへ送られる。図４は、図２に示す従来の画像データ圧縮方法と図３に示す従来のデータ暗号化方法とを縦続接続し、画像データ暗号化方法を実現した従来の一構成例を示すブロック図である。この画像データ暗号化方法では、入力端子４１から入力された画像データを、図２の画像データ圧縮方法４２で圧縮した後、図３のデータ暗号化方法４３で暗号化し、その結果を出力端子４４から出力する。

【０００５】

【発明が解決しようとする課題】しかしながら、上記構成の画像データ暗号化方法では、画像データ圧縮方法４２で圧縮された画像データの全てをデータ暗号化方法４３で暗号化する必要があるため、暗号化のための処理量が大きくなるという問題がある。これを防止するため、圧縮された画像データの一部を暗号化することも考えられるが、暗号強度が劣化するという欠点があり、未だ技術的十分満足のゆく画像データ暗号化方法を得ることが困難であった。本発明は、前記従来技術が持っていた課題として、暗号強度を犠牲にすることなく、暗号化のための処理量を低減することが困難な点について解決した画像データ暗号化方法を提供するものである。

【０００６】

【課題を解決するための手段】第１の発明は、前記課題を解決するために、圧縮した画像データを暗号化する画像データ暗号化方法において、２次元の画像信号をｎ画素ｘｎ画素のブロックに分割する分割処理と、前記分割処理で分割されたブロックをＤＣＴ変換するＤＣＴ処理と、前記ＤＣＴ処理の出力のうちの直流成分を量子化する直流量子化処理と、前記ＤＣＴ処理の出力のうちの交流成分を量子化する交流量子化処理と、前記直流量子化処理の出力を暗号化する暗号化処理とを実行する。さらに、前記交流量子化処理の出力をエントロピー符号化する交流エントロピー符号化処理と、前記暗号化処理の出力と前記交流エントロピー符号化処理の出力とを多重化する多重化処理とを、実行するようにしている。第２の発明では、第１の発明の画像データ暗号化方法において、前記直流量子化処理では、出力信号をｎビットの固定長符号に符号化する固定長符号化処理を行い、前記暗号化処理では、前記直流量子化処理の出力に対してｎビット毎に暗号化し、前記多重化処理では、１ブロック毎に前記暗号化処理の出力と前記交流エントロピー符号化処理の出力を多重化するようにしている。第３の発明では、圧縮した画像データを暗号化する画像データ暗号化方法において、２次元の画像信号をｎ画素ｘｎ画素のブロックに分割する分割処理と、前記分割処理で分割されたブロックをＤＣＴ変換するＤＣＴ処理と、前記ＤＣＴ処理の出力のうちの直流成分を差動符号化する差動符号化処理と、前記差動符号化処理の出力を量子化する直流量子化処理と、前記直流量子化処理の出力をエントロピー符号化する直流エントロピー符号化処理と、前記直流エントロピー符号化処理の出力を暗号化する暗号化処理とを実行する。さらに、前記ＤＣＴ処理の出力のうちの交流成分を量子化する交流量子化処理と、前記交流量子化処理の出力をエントロピー符号化する交流エントロピー符号化処理と、１画面分の前記暗号化処理の出力ビット数をカウントし、そのカウント値と１画面分の前記暗号化処理の出力と１画面分の前記交流エントロピー符号化処理の出力とを多重化する多重化処理とを、実行するようにしている。

【０００７】

【作用】第１の発明によれば、以上のように画像データ暗号化方法を構成したので、画像信号が入力されると、ブロック処理でブロックに分割され、その分割されたブロックがＤＣＴ処理でＤＣＴ変換され、直流成分と交流成分が出力される。直流成分は、直流量子化処理で量子化され、暗号化処理で暗号化されて多重化処理へ送られる。ＤＣＴ処理で出力された交流成分は、交流量子化処理で量子化され、交流エントロピー符号化処理でエントロピー符号化されて多重化処理へ送られる。多重化処理では、暗号化処理の出力と交流エントロピー符号化処理の出力とを多重化する。このように、画像データのうちの直流成分だけを暗号化する。

【０００８】一般に、データを圧縮すると、長さが一定でない符号が出力される。圧縮したデータの一部分を暗号化する場合、どこからどこまでが暗号化されているのかが、復号化側でわかる必要がある。第１の発明の場合には、多重化後にどこが直流成分で、どこが交流成分かを判別する必要がある。そこで、第２の発明では、直流成分を固定長にすることにより、直流成分と交流成分の判別を行うようにしている。即ち、第２の発明では、ＤＣＴ処理によって処理された直流成分が、直流量子化処理において該直流成分が量子化され、それが固定長符号

に符号化され、それらのｎビット毎に暗号化処理で暗号化され、多重化処理へ送られる。多重化処理では、１ブロック毎に暗号化処理の出力と交流エントロピー符号化処理の出力を多重化する。このように、直流成分が固定長で符号化されているので、受信側で直流成分の終了の検出が可能となる。

【０００９】第３の発明では、直流成分のビット数を付加情報として伝送することにより、前記の直流成分と交流成分の判別を行っている。即ち、この第３の発明では、画像信号が入力されると、分割処理でブロックに分割され、その分割されたブロックがＤＣＴ処理でＤＣＴ変換され、直流成分と交流成分が出力される。直流成分は、差動符号化処理で差動符号化され、直流エントロピー符号化処理でエントロピー符号化され、暗号化処理で暗号化されて多重化処理へ送られる。ＤＣＴ処理によって出力された交流成分は、交流量子化処理で量子化され、交流エントロピー符号化処理でエントロピー処理された後、多重化処理へ送られる。多重化処理では、１画面分の暗号化処理の出力ビット数をカウントし、そのカウント値と１画面分の交流エントロピー符号化処理の出力とを多重化する。この多重化された出力の先頭に直流成分のビット長が固定長符号化されているので、受信側で直流成分の終了の検出が可能となる。従って、前記課題を解決できるのである。

【００１０】

【実施例】

第１の実施例

図１は、本発明の第１の実施例を示す画像データ暗号化方法の構成ブロック図である。この画像データ暗号化方法では、例えば入力端子１０１より入力された１画素８ビットからなる信号が、ブロック化部１０２において縦８画素、横８画素のブロックに分割され、ＤＣＴ部１０３へ送られる。ＤＣＴ部１０３は、ブロック化部１０２からのブロックをＤＣＴ変換し、直流成分ｆ（０，０）のデータ、及び交流成分ｆ（ｉ，ｊ）のデータを出力する。この直流成分ｆ（０，０）は、直流量子化部１０４において所定のステップサイズＱＵＡＮＴ（０，０）で量子化され、その量子化出力ｑ（０，０）が暗号化部１１０で暗号化された後、該暗号化データが多重化部１３１へ送られる。ＤＣＴ部１０３から出力された交流成分ｆ（ｉ，ｊ）は、交流量子化部１０５において所定のステップサイズＱＵＡＮＴ（ｉ，ｊ）で量子化され、その量子化出力ｑ（ｉ，ｊ）が交流エントロピー符号化部１２０においてジグザクスキャン等によってエントロピー符号化され、多重化部１３１へ送られる。多重化部１３１では、暗号化部１１０及び交流エントロピー符号化部１２０の出力を多重化し、固定長で符号化された直流成分ＤＣと可変長符号化された交流成分ＡＣとが、繰り返されて生成された暗号化データが、出力端子１３２から出力される。この暗号化されたデータは、直流成分ＤＣが固定長で符号化されているので、該データが暗号化されていても、受信側で各成分の終了を検出でき、正しく復号化することが可能となる。

【００１１】次に、図１の各ブロックにおける処理内容を図５～図１６を参照しつつ説明する。図５は、図１のブロック化部１０２の処理内容の説明図である。本実施例では、例えば縦２８８画素、横３５２画素からなる画像信号を例にとって説明する。図１の入力端子１０１から入力された縦２８８画素、横３５２画素からなる画像信号ｘ（ｉ，ｊ）は、図１のブロック化部１０２で、図５に示すように縦３６個、横４４個のブロックに分割される。

【００１２】図６は、ブロック化部１０２で分割されたブロックのうちの１つのブロックｂ（ｋ，ｌ）の説明図である。１つのブロックｂ（ｋ，ｌ）は、図６に示すように、６４画素から構成される。３６×４４＝１５８４個のブロックは、１個ずつ順に図１のＤＣＴ部１０３へ入力される。入力される順序は任意であるが、本実施例では例えば、ｂ（０，０），ｂ（０，１），ｂ（０，２），・・・・・・・・，ｂ（０，４３），ｂ（１，０），ｂ（１，１），・・・・・・・・，ｂ（３５，４２），ｂ（３５，４３）の順に入力するものとする。図１のＤＣＴ部１０３では、ブロック化部１０２からのブロックをＤＣＴ変換し、直流成分ｆ（０，０）のデータ、及び交流成分ｆ（ｉ，ｊ）のデータを出力する。

【００１３】図７は、図１のＤＣＴ部１０３におけるＤＣＴ変換の説明図である。例えば、６４画素からなる入力データをｅ（ｉ，ｊ）（ｉ＝０～７，ｊ＝０～７）とすると図１のＤＣＴ部１０３では次式の演算を行い、出力データｆ（ｕ，ｖ）（ｕ＝０～７，ｖ＝０～７）を出力する。

【００１４】

【数１】

$$f(u,v)=\frac{1}{4}C(u)\cdot C(v)\sum_{i=0}^{7}\sum_{j=0}^{7}e(i,j)\cdot\cos\left(\frac{\Pi u(2i+1)}{16}\right)\cdot\cos\left(\frac{\Pi v(2j+1)}{16}\right)$$

但し、

$$c(u)=\begin{cases}\frac{1}{\sqrt{2}} & u=0\\ 1 & u\neq 0\end{cases}$$

f（0，0）：直流成分

f（0，0）以外のf（i，j）：交流成分

図1のDCT部103から出力された直流成分f（0，0）は、直流量子化部104において次式に従い所定のステップサイズQUANT（0，0）で量子化され、その量子化出力q（0，0）が図1の暗号化部110へ送られる。

q（0，0）＝int［f（0，0）／QUANT（0，0）］

ここで、int［ ］は小数点以下を四捨五入する整数化を表す。例えば、f（0，0）は8ビットであるので、QUANT（0，0）＝8の場合には、量子化出力q（0，0）が5ビットとなる。この量子化出力q（0，0）は、図1の暗号化部110で暗号化される。

【0015】図8は、図1の暗号化部110の構成ブロック図である。この図では、前記文献2に記載されている64ビット入力、64ビット出力の暗号化方法を5ビットCFB（Cipher Feed Back）モードで用いている。この暗号化部110は、5ビットの直流成分f（0，0）のデータを入力する入力端子111－1～111－5と、初期値を設定する64ビットのシフトレジスタ112とを備え、該シフトレジスタ112の出力側が暗号化部113を介して64ビットのレジスタ114に接続されている。このシフトレジスタ114の出力側と入力端子111－1～111－5は、排他的論理和ゲート115－1～115－6に接続されている。排他的論理和ゲート115－1～115－6の出力側には、パラレル／シリアル変換回路（以下、P／S変換回路という）116と、5ビットの暗号化データを出力する出力端子117－1～117－5とが接続され、該P／S変換回路116の出力側がシフトレジスタ112に接続されている。64ビットのシフトレジスタ112には初期値が設定されており、その初期値が符号化部113で符号化され、その符号化された64ビットのデータがレジスタ114に格納される。入力端子111－1～111－5から入力される5ビットの直流成分f（0，0）のデータは、排他的論理和ゲート115－1～115－6において、レジスタ114のうちの例えば左端から5ビットとそれぞれ排他的論理和がとられ、5ビットの暗号化データが出力端子117－1～117－5へ出力される。また、この5ビットの暗号化データは、P／S変換回路116においてシリアルデータに変換され、シフトレジスタ112に入力され、該シフトレジスタ112の内容が5ビット右方向へシフトされる。このシフト結果は、暗号化部113で暗号化され、次のブロックの直流成分f（0，0）のデータを暗号化するために用いられる。出力端子117－1～117－5から出力された5ビットの暗号化データは、図1の多重化部131へ送られる。

【0016】一方、図1のDCT部103から出力された交流成分f（i，j）のデータは、交流量子化部105において次式に従いステップサイズQUANT（i，j）で量子化され、その量子化出力q（i，j）が交流エントロピー符号化部120へ送られる。

q（i，j）＝int［f（i，j）／QUANT（i，j）］

図9は、図1のエントロピー符号化部120の構成ブロック図である。この交流エントロピー符号化部120は、交流量子化部105からの量子化出力q（i，j）を入力する入力端子121を有し、それにはジグザグスキャン部122を介してゼロ判定部123が接続されて

いる。ゼロ判定部１２３の出力側には、ランレングスカウント部１２４及びグループ化部１２５が接続され、そのランレングスカウント部１２４及びグループ化部１２５の出力側に、２次元ハフマン符号化部１２６が接続されている。さらに、２次元ハフマン符号化部１２６の出力側とグループ化部１２５の出力側には、多重化部１２７が接続され、さらにその出力側に出力端子１２８が接続されている。入力端子１２１より入力された交流成分の量子化出力ｑ（ｉ，ｊ）は、ジグザグスキャン部１２２に入力される。図１０は、図９のジグザグスキャン部１２２の説明図である。ジグザグスキャン部１２２では、図１０に示すように、矢印の方向に交流成分ｆ（ｉ，ｊ）のデータをスキャンし、２次元のｆ（ｉ，ｊ）を１次元に並び換える。このジグザグスキャン部１２２の出力は、例えば、ｆ（０，１），ｆ（１，０），ｆ（２，０），ｆ（１，１），ｆ（０，２），ｆ（０，３），・・・・・・・・，ｆ（７，７）のような順序になり、図９のゼロ判定部１２３へ入力される。

【００１７】ゼロ判定部１２３では、入力された交流成分ｆ（ｉ，ｊ）のデータがゼロであるかどうかを判定する。ゼロである場合には、ランレングスカウント部１２４においてカウンタの値が＋１増分され、そのゼロの連続の数（ラン）Ｎが２次元ハフマン符号化部１２６へ送られる。ゼロ判定部１２３においてゼロでないと判定された場合には、交流成分ｆ（ｉ，ｊ）のデータがグループ化部１２５においてグループ番号Ｓと付加ビットＤが求められ、そのグループ番号Ｓが２次元ハフマン符号化部１２６へ送られると共に、該付加ビットＤが多重化部１２７へ送られる。図１１は、交流成分ｆ（ｉ，ｊ）とグループ番号Ｓ及び付加ビットＤの関係を示す図である。例えば、入力された交流成分ｆ（ｉ，ｊ）＝－２の場合には、グループ番号Ｓ＝２、付加ビットＤ＝１０となる。グループ化部１２５よりグループ番号Ｓが２次元ハフマン符号化部１２６へ送られると、該２次元ハフマン符号化部１２６には、ランレングスカウント部１２４より現在までのランＮが入力される。ランレングスカウント部１２４の内部のカウンタは、次のゼロランの数をカウントするために、ゼロにリセットされる。図１２、図１３、及び図１４は、２次元ハフマン符号化部１２６で用いられるハフマン符号化テーブルの例を示す図である。２次元ハフマン符号化部１２６では、図１２～図１４に示すハフマン符号化テーブルに基づき、ランＮとグループ番号Ｓからハフマン符号化を行い、符号化されたコードＣを多重化部１２７へ出力する。例えば、ランＮ＝５、グループ番号Ｓ＝２の場合には、２次元ハフマン符号化部１２６からコードＣ＝１１１１１１０１１１が出力され、多重化部１２７へ送られる。多重化部１２７では、２次元ハフマン符号化部１２６からのコードＣとグループ化部１２５からの付加ビットＤとを直列に並べて多重化し、その出力データを出力端子１２８から出力して図１の多重化部１３１へ送る。これら一連の動作が、ｆ（７，７）までの全ての交流成分がジグザグスキャン部１２２より入力されるまで繰り返される。例えば、図１の交流量子化部１０５からの入力系列が１，０，０，０，０，０，－２，・・・・・・であるとき、図１の多重化部１３１への出力は、０００１１１１１１１０１１１１０・・・・・・となる。図１５は、この例の場合の交流エントロピー符号化部１２０の動作説明図である。

【００１８】図１の交流エントロピー符号化部１２０では、図１５に示すように、最初の１が図９のジグザグスキャン部１２２から入力されると、それまでのゼロランの数Ｎ＝０、図１１より１のグループ番号Ｓ＝１であるので、図１２～図１４より、コードＣ＝００が図９の多重化部１２７へ出力される。引き続き、図１１より、１の付加コードＤ＝０が図９の多重化部１２７へ出力される。次に、５個の０に引き続いて－２が入力されるので、Ｎ＝５、Ｓ＝２でＣ＝１１１１１１１０１１１、Ｄ＝１０が図９の多重化部１２７へ出力される。このような図１の交流エントロピー符号化部１２０の出力が多重化部１３１に入力され、該多重化部１３１において暗号化部１１０の出力とブロック毎に多重化され、出力端子１３２から出力される。図１６に、出力端子１３２からの出力信号のフォーマットを示す。このフォーマットでは、５ビットの固定長で符号化された直流成分ＤＣと、可変長符号化された交流成分ＡＣが、１５８４ブロック繰り返される。このように、直流成分ＤＣが固定長で符号化されているので、入力画像データが符号化されていても、受信側で各成分の終了を検出でき、正しく復号化することが可能となる。以上のように、本実施例では、直流成分ｆ（０，０）だけを暗号化部１１０で暗号化するようにしたので、暗号強度を犠牲にすることなく、暗号化のための処理量を低減できる。例えば、３５２画素×２８８画素からなる約２．５Mibtの画像データを扱う場合、従来の図４の画像データ暗号化方法では、約７０Kbitのデータを暗号化しなければならないのに対し、本実施例を用いると、約６Kbitのデータを暗号化するだけでよい。そのため、暗号化のための処理量が約１／１０に低減できる。

【００１９】第２の実施例

図１７は、本発明の第２の実施例を示す画像データ暗号化方法の構成ブロック図であり、第１の実施例を示す図１中の要素と共通の要素には共通の符号が付されている。この画像データ暗号化方法では、図１のＤＣＴ部１０３の出力側と直流量子化部１０４の入力側との間に、直流成分ｆ（０，０）を差動符号化する差動符号化部１４０が接続されている。さらに、図１の直流量子化部１０４の出力側に、エントロピー符号化を行って可変長符号化を施す直流エントロピー符号化部１５０と、該直流エントロピー符号化部１５０の出力を暗号化する暗号化

部１６０とを介して、多重化部１７０が接続されている。多重化部１７０は、暗号化部１６０の出力と交流エントロピー符号化部１２０の出力とを多重化し、それを出力端子１３２から出力する機能を有している。この画像データ符号化方法では、画像信号が入力端子１０１から入力されると、それがブロック化部１０２でブロックに分割され、分割されたブロックがＤＣＴ部１０３でＤＣＴ変換され、直流成分ｆ（０，０）のデータ及び交流成分ｆ（ｉ，ｊ）のデータが出力される。ＤＣＴ部１０３から出力された直流成分ｆ（０，０）のデータは、差動符号化部１４０において前ブロックの直流成分との差が求められ、その差が直流量子化部１０４で量子化され、直流エントロピー符号化部１５０でエントロピー符号化された後、暗号化部１６０で暗号化されて多重化部１７０へ送られる。

【００２０】一方、ＤＣＴ部１０３から出力された交流成分ｆ（ｉ，ｊ）のデータは、第１の実施例と同様に、交流量子化部１０５で量子化され、交流エントロピー符号化部１２０でエントロピー符号化された後、多重化部１７０へ送られる。多重化部１７０では、暗号化部１６０の出力と交流エントロピー符号化部１２０の出力とを多重化し、出力端子１３２から出力する。次に、図１７の各ブロックの処理を、図１８～図２１を参照しつつ説明する。図１８は、図１７の直流エントロピー符号化部１５０の内部構成を示すブロック図である。この直流エントロピー符号化部１５０は、図１７の直流量子化部１０４の出力を入力する入力端子１５１を有し、それにはグループ化部１５２が接続されている。グループ化部１５２は、入力端子１５１の入力をグループ化し、グループ番号Ｓ及び付加ビットＤを出力する機能を有し、該グループ番号Ｓが１次元ハフマン符号化部１５３へ、該付加ビットＤが多重化部１５４へ送られる。１次元ハフマン符号化部１５３は、グループ番号Ｓに基づきハフマン符号化を行い、コードＣを多重化部１５４へ出力する機能を有している。多重化部１５４は、コードＣと付加ビットＤを多重化して出力端子１５５へ出力する機能を有している。図１８の直流エントロピー符号化部１５０において、図１７の直流量子化部１０４の出力が入力端子１５１より入力され、その入力データがグループ化部１５２においてグループ化され、グループ番号Ｓが１次元ハフマン符号化部１５３へ、付加ビットＤが多重化部１５４へ送られる。グループ化部１５２では、例えば図１１と同一のデータに基づき、グループ化処理を行う。１次元ハフマン符号化部１５３は、例えば図１９に示すハフマン符号化テーブルを用い、入力されたグループ番号Ｓをハフマン符号化により可変長符号化し、コードＣを多重化部１５４へ出力する。例えば、グループ番号Ｓ＝５のときには、図１９に示すように、コードＣ＝１１０が出力される。多重化部１５４は、コードＣと付加ビットＤを多重化し、その直列データを出力端子１５５を介して図１７の暗号化部１６０へ出力する。

【００２１】図１７の暗号化部１６０では、例えば前記文献２に記載された方法により、直流エントロピー符号化部１５０より入力されるデータを６４ビット毎にブロック化して暗号化し、多重化部１７０へ送る。なお、第１の実施例を示す図１の暗号化部１１０と同様に、ＣＦＢモードを用いて暗号化することも可能である。ＤＣＴ部１０３から出力された交流成分ｆ（ｉ，ｊ）のデータは、第１の実施例と同様に、交流量子化部１０５で量子化され、交流エントロピー符号化部１２０でエントロピー符号化された後、多重化部１７０へ送られる。図２０は、図１７の多重化部１７０の内部構成を示すブロック図である。この多重化部１７０は、図１７の暗号化部１６０の出力を入力する入力端子１７１と、交流エントロピー符号化部１２０の出力を入力する入力端子１７２とを備え、それらの入力端子１７１，１７２にデータ一時格納用のバッファ１７３，１７４が接続されている。バッファ１７３の出力側には、ビット数カウント部１７５及び多重化部１７６が接続され、さらにバッファ１７４の出力側が該多重化部１７６に接続され、該多重化部１７６の出力側に出力端子１３２が接続されている。この多重化部１７０では、入力端子１７１，１７２より入力された図１７の暗号化部１６０及び交流エントロピー符号化部１２０の出力データが、バッファ１７３，１７４に１画面１５８４ブロック分が蓄積される。１画面分がバッファ１７３，１７４にそれぞれ蓄積されると、該バッファ１７３に蓄積された直流成分の暗号化されたデータが、ビット数カウント部１７５へ送られる。ビット数カウント部１７５は、バッファ１７３に蓄積されたビット数をカウントし、多重化部１７６へ送る。多重化部１７６は、バッファ１７３の出力データとバッファ１７４の出力データを多重化し、出力端子１３２へ出力する。図２１は、図１７及び図２０の出力端子１３２から出力される出力信号のフォーマットである。先頭に直流成分ＤＣのビット長を固定長符号化しているので、受信側で直流成分ＤＣの終了を検出でき、正しく復号できる。

【００２２】以上のように、本実施例では、ＤＣＴ部１０３から出力された直流成分ｆ（０，０）に対し、差動符号化部１４０で差動符号化を行い、直流エントロピー符号化部１５０でエントロピー符号化を行い、可変長符号化を施している。この場合、直流成分ｆ（０，０）が暗号化部１６０で暗号化されても、受信側で直流成分ＤＣの終わりが検出できるように、例えば１５８４ブロック全体の直流成分ＤＣを多重化部１７０内のバッファ１７３，１７４に蓄えて該直流成分ＤＣの長さをビット数カウント部１７５でカウントし、その長さを出力端子１３２からの出力系列の先頭に固定長符号で付加している。そのため、受信側で直流成分の終了を検出でき、正しく復号できるので、第１の実施例と同様に、暗号強度を犠牲にすることなく、暗号化のための処理量を低減で

きる。

【００２３】なお、本発明は上記実施例に限定されず、例えば、図１の暗号化部１１０、及び交流エントロピー符号化部１２０を、図８及び図９以外の構成で処理することも可能である。同様に、図１７の直流エントロピー符号化部１５０、及び多重化部１７０を、図１８及び図２０以外の構成で処理することも可能である。

【００２４】

【発明の効果】以上詳細に説明したように、第１の発明によれば、画像データの最も重要な情報を含む直流成分だけを暗号化するようにしたので、暗号強度を犠牲にすることなく、暗号化のための処理量を低減することができる。第２の発明によれば、直流成分が固定長で符号化されるので、入力画像信号が暗号化されていても、受信側で直流成分と交流成分の終了を検出でき、正しく復号化することが可能となる。特に、受信ブロック毎に復号を開始できる効果がある。第３の発明によれば、直交変換された直流成分に差動符号化やエントロピー符号化を用いて可変長符号化を施している。この際、多重化処理において暗号化処理の出力ビット数をカウントし、そのカウント値を交流エントロピー符号化処理の出力に固定長符号で付加しているので、直流成分が暗号化されても、受信側で直流成分の終了を検出でき、正しく復号化することが可能となる。また、この第３の発明では、１画面全体を受信した後でないと、全体の復号が始められないが、可変長符号化しているので、第２の発明よりも圧縮効率が向上する。

【図面の簡単な説明】

【図１】本発明の第１の実施例を示す画像データ暗号化方法の構成ブロック図である。

【図２】従来の画像データ圧縮方法の構成ブロック図である。

【図３】従来のデータ暗号化方法の構成ブロック図である。

【図４】従来の画像データ暗号化方法の構成ブロック図である。

【図５】図１のブロック化部の説明図である。

【図６】図１のブロック化データの説明図である。

【図７】図１のＤＣＴ変換の説明図である。

【図８】図１の暗号化部の構成ブロック図である。

【図９】図１の交流エントロピー符号化部の構成ブロック図である。

【図１０】図９のジグザグスキャン部の説明図である。

【図１１】図９の交流成分ｆ（ｉ，ｊ）とグループ番号Ｓ及び付加ビットＤの関係を示す図である。

【図１２】図９の２次元ハフマン符号化部で用いるハフマン符号化テーブルを示す図である。

【図１３】図９の２次元ハフマン符号化部で用いるハフマン符号化テーブルを示す図である。

【図１４】図９の２次元ハフマン符号化部で用いるハフマン符号化テーブルを示す図である。

【図１５】図１のエントロピー符号化部の説明図である。

【図１６】図１の多重化部における出力信号のフォーマットを示す図である。

【図１７】本発明の第２の実施例を示す画像データ暗号化方法の構成ブロック図である。

【図１８】図１７の直流エントロピー符号化部の構成ブロック図である。

【図１９】図１８の１次元ハフマン符号化部で用いるハフマン符号化テーブルを示す図である。

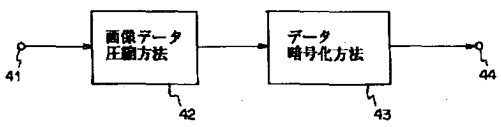
【図２０】図１７の多重化部の構成ブロック図である。

【図２１】図１７の多重化部における出力信号のフォーマットを示す図である。

【符号の説明】

１０２	ブロック化部
１０３	ＤＣＴ部
１０４	直流量子化部
１０５	交流量子化部
１１０，１６０	暗号化部
１２０	交流エントロピー符号化部
１３１，１７０	多重化部
１４０	差動符号化部
１５０	直流エントロピー符号化部

【図４】



従来の画像データ暗号化方法

【図１５】

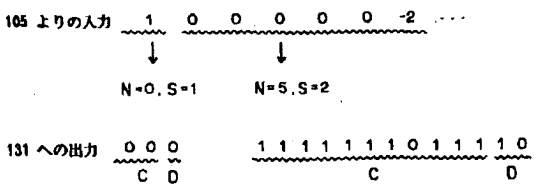
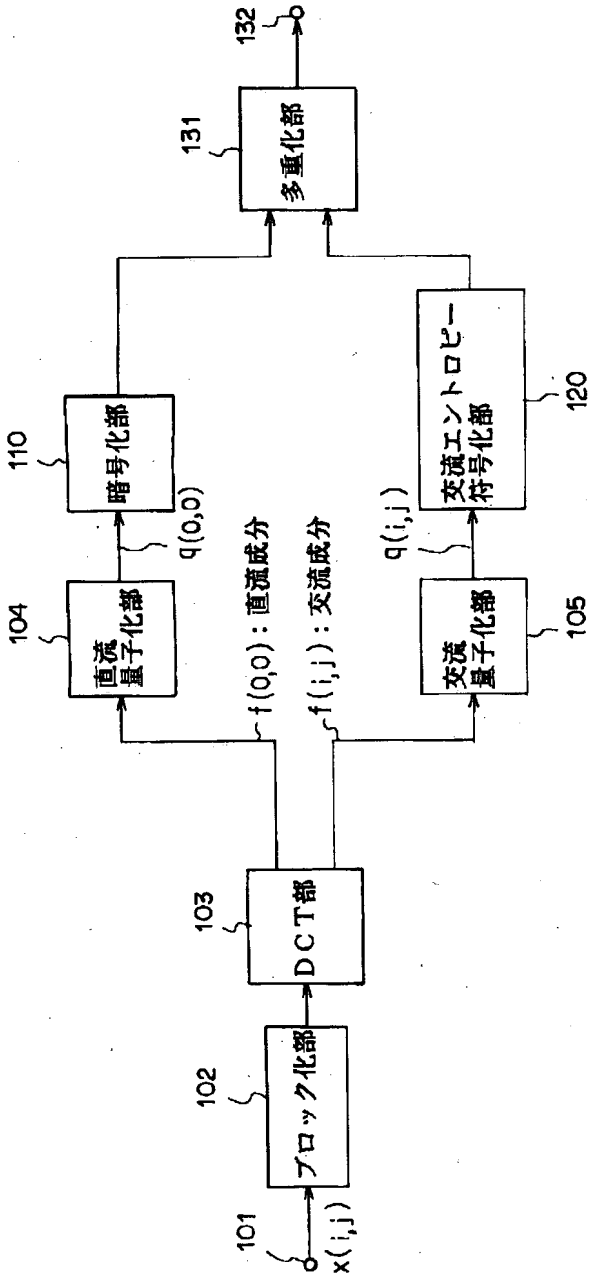


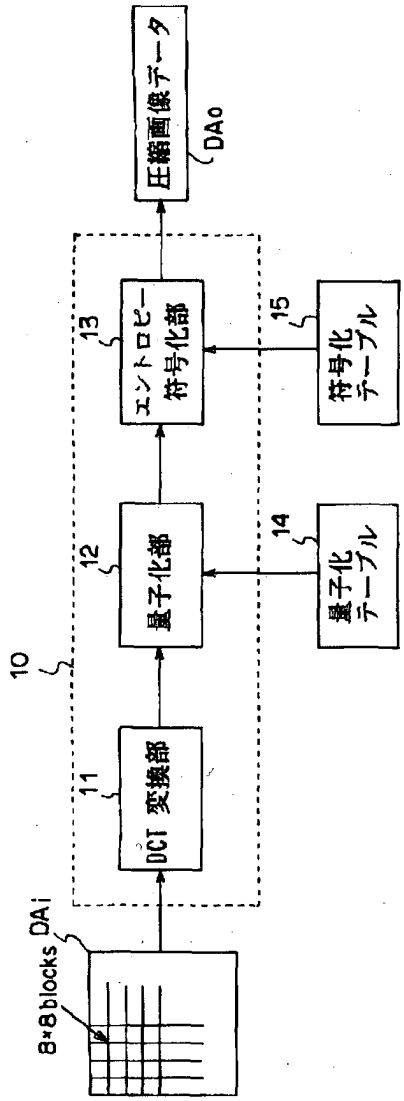
図１のエントロピー符号化部

【図1】



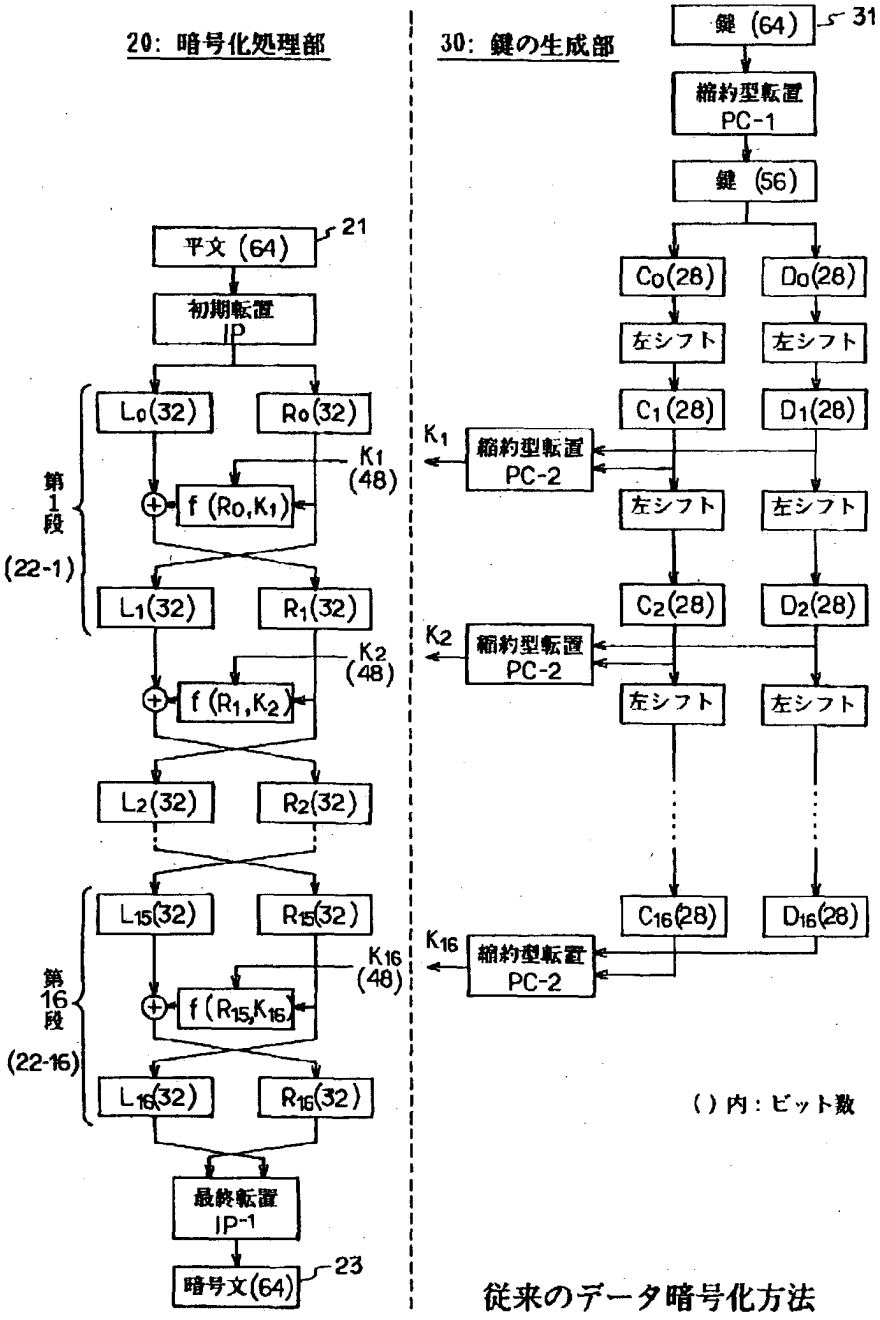
本発明の第１の実施例の画像データ暗号化方法

【図2】



従来の画像データ圧縮方法

【図3】



従来のデータ暗号化方法

【図5】

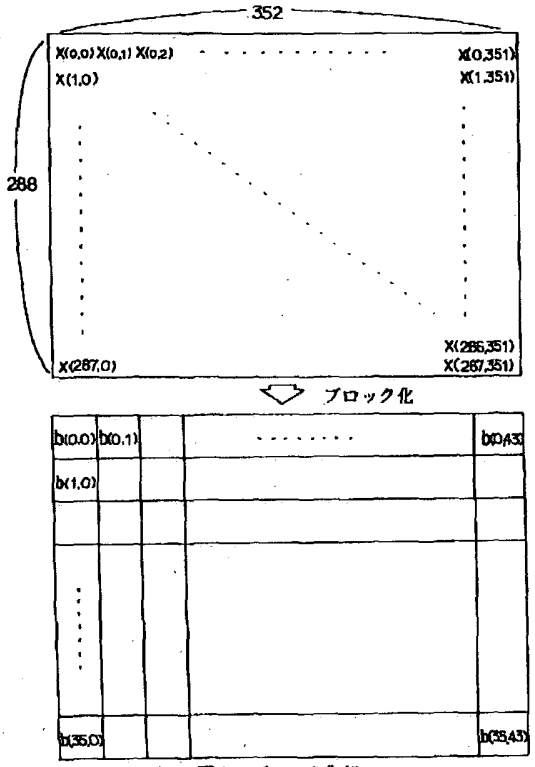


図1のブロック化部

【図6】

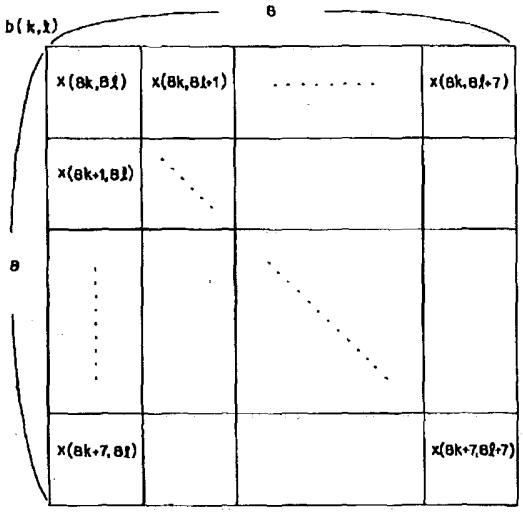


図1のブロック化データ

【図8】

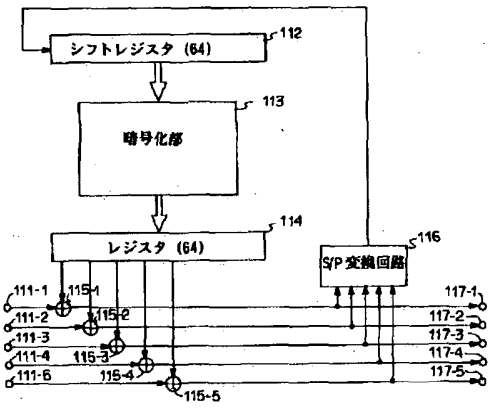


図1の暗号化部

【図10】

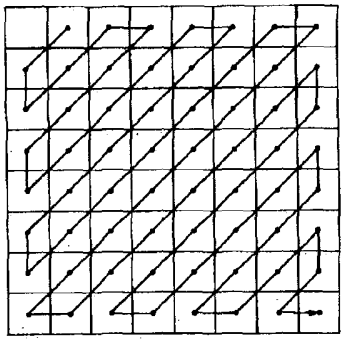


図9のジグザグスキャン部

【図7】

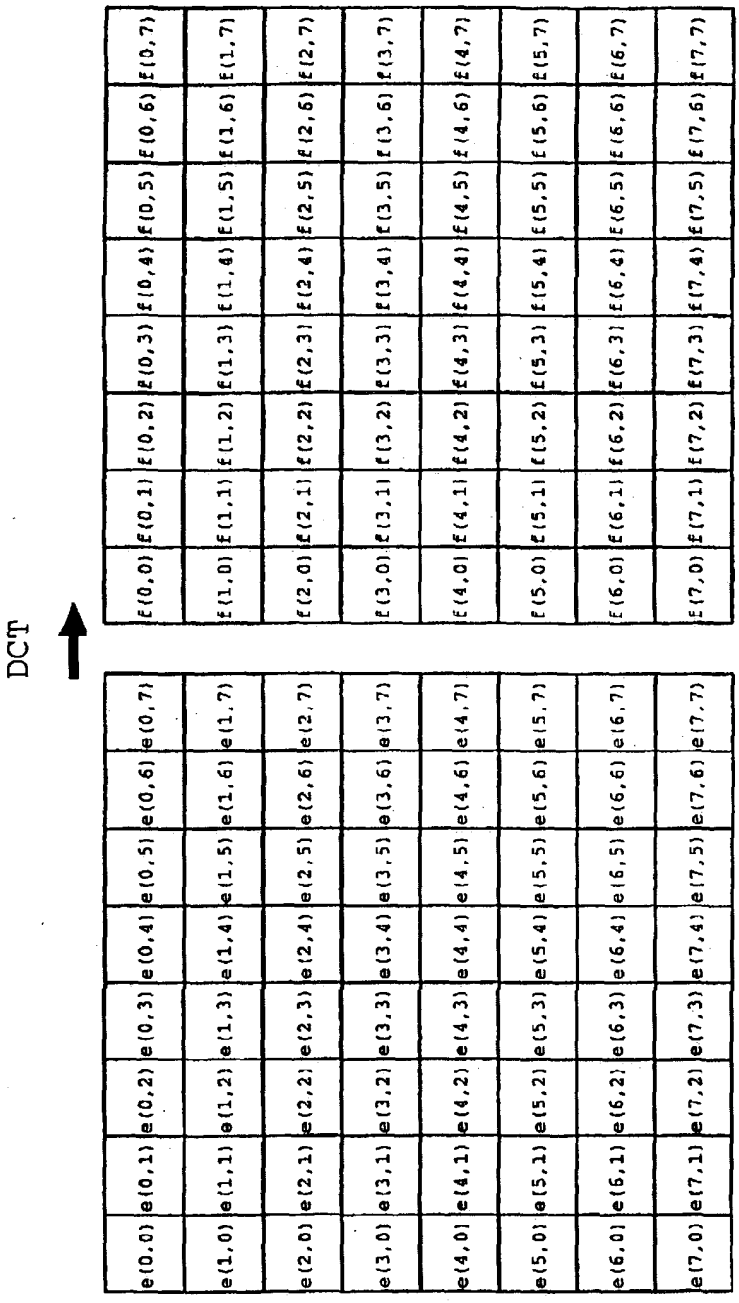

DCT
e(0,0) e(0,1) e(0,2) e(0,3) e(0,4) e(0,5) e(0,6) e(0,7)
e(1,0) e(1,1) e(1,2) e(1,3) e(1,4) e(1,5) e(1,6) e(1,7)
e(2,0) e(2,1) e(2,2) e(2,3) e(2,4) e(2,5) e(2,6) e(2,7)
e(3,0) e(3,1) e(3,2) e(3,3) e(3,4) e(3,5) e(3,6) e(3,7)
e(4,0) e(4,1) e(4,2) e(4,3) e(4,4) e(4,5) e(4,6) e(4,7)
e(5,0) e(5,1) e(5,2) e(5,3) e(5,4) e(5,5) e(5,6) e(5,7)
e(6,0) e(6,1) e(6,2) e(6,3) e(6,4) e(6,5) e(6,6) e(6,7)
e(7,0) e(7,1) e(7,2) e(7,3) e(7,4) e(7,5) e(7,6) e(7,7)
E(0,0) E(0,1) E(0,2) E(0,3) E(0,4) E(0,5) E(0,6) E(0,7)
E(1,0) E(1,1) E(1,2) E(1,3) E(1,4) E(1,5) E(1,6) E(1,7)
E(2,0) E(2,1) E(2,2) E(2,3) E(2,4) E(2,5) E(2,6) E(2,7)
E(3,0) E(3,1) E(3,2) E(3,3) E(3,4) E(3,5) E(3,6) E(3,7)
E(4,0) E(4,1) E(4,2) E(4,3) E(4,4) E(4,5) E(4,6) E(4,7)
E(5,0) E(5,1) E(5,2) E(5,3) E(5,4) E(5,5) E(5,6) E(5,7)
E(6,0) E(6,1) E(6,2) E(6,3) E(6,4) E(6,5) E(6,6) E(6,7)
E(7,0) E(7,1) E(7,2) E(7,3) E(7,4) E(7,5) E(7,6) E(7,7)

図1のDCT 変換

【図9】

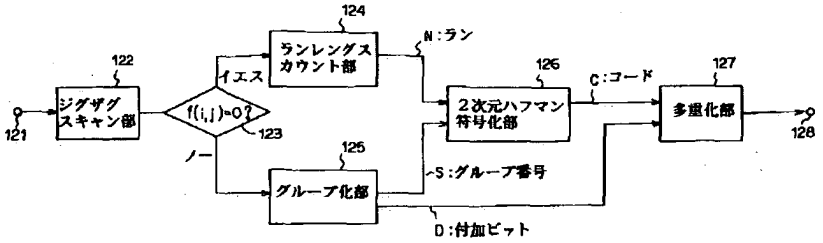


図1の交流エントロピー符号化部

【図11】

f(i,j)	グループ番号 S	付加ビット D
−32767	15	1111111111111111
−32766		1111111111111110
⋮		⋮
−16384		1000000000000000
−16383	14	1111111111111111
⋮		⋮
		1000000000000000
⋮		⋮
−3	2	11
−2		10
−1	1	1
0	0	なし
1	1	0
⋮		⋮
16384	15	0000000000000000
32767		0111111111111111
32768	16	なし

交流成分 f(i,j) とグループ番号S 及び付加ビットD の関係

【図12】

N/S	符号長	C
0/0(EOB)	4	1010
0/1	2	00
0/2	2	01
0/3	3	100
0/4	4	1011
0/5	5	11010
0/6	7	1111000
0/7	8	11111000
0/8	10	1111110110
0/9	16	1111111110000010
0/A	16	1111111110000011
1/1	4	1100
1/2	5	11011
1/3	7	1111001
1/4	9	111110110
1/5	11	11111110110
1/6	16	1111111110000100
1/7	16	1111111110000101
1/8	16	1111111110000110
1/9	16	1111111110000111
1/A	16	1111111110001000
2/1	5	11100
2/2	8	11111001
2/3	10	1111110111
2/4	12	111111110100
2/5	16	1111111110001001
2/6	16	1111111110001010
2/7	16	1111111110001011
2/8	16	1111111110001100
2/9	16	1111111110001101
2/A	16	1111111110001110
3/1	6	111010
3/2	9	111110111
3/3	12	111111110101
3/4	16	1111111110001111
3/5	16	1111111110010000
3/6	16	1111111110010001
3/7	16	1111111110010010
3/8	16	1111111110010011
3/9	16	1111111110010100
3/A	16	1111111110010101
4/1	6	111011
4/2	10	1111111000
4/3	16	1111111110010110
4/4	16	1111111110010111
4/5	16	1111111110011000
4/6	16	1111111110011001
4/7	16	1111111110011010
4/8	16	1111111110011011
4/9	16	1111111110011100
4/A	16	1111111110011101
5/1	7	1111010
5/2	11	11111110111
5/3	16	1111111110011110

ハフマン符号化テーブル

【図１３】

N/S	符号長	C
5/4	16	1111111110011111
5/5	16	1111111110100000
5/6	16	1111111110100001
5/7	16	1111111110100010
5/8	16	1111111110100011
5/9	16	1111111110100100
5/A	16	1111111110100101
6/1	7	1111011
6/2	12	111111110110
6/3	16	1111111110100110
6/4	16	1111111110100111
6/5	16	1111111110101000
6/6	16	1111111110101001
6/7	16	1111111110101010
6/8	16	1111111110101011
6/9	16	1111111110101100
6/A	16	1111111110101101
7/1	8	11111010
7/2	12	111111110111
7/3	16	1111111110101110
7/4	16	1111111110101111
7/5	16	1111111110110000
7/6	16	1111111110110001
7/7	16	1111111110110010
7/8	16	1111111110110011
7/9	16	1111111110110100
7/A	16	1111111110110101
8/1	9	111111000
8/2	15	111111111000000
8/3	16	1111111110110110
8/4	16	1111111110110111
8/5	16	1111111110111000
8/6	16	1111111110111001
8/7	16	1111111110111010
8/8	16	1111111110111011
8/9	16	1111111110111100
8/A	16	1111111110111101
9/1	9	111111001
9/2	16	1111111110111110
9/3	16	1111111110111111
9/4	16	1111111111000000
9/5	16	1111111111000001
9/6	16	1111111111000010
9/7	16	1111111111000011
9/8	16	1111111111000100
9/9	16	1111111111000101
9/A	16	1111111111000110
A/1	9	111111010
A/2	16	1111111111000111
A/3	16	1111111111001000
A/4	16	1111111111001001
A/5	16	1111111111001010
A/6	16	1111111111001011
A/7	16	1111111111001100

ハフマン符号化テーブル

【図１４】

N/S	符号長	C
A/8	16	1111111111001101
A/9	16	1111111111001110
A/A	16	1111111111001111
B/1	10	1111111001
B/2	16	1111111111010000
B/3	16	1111111111010001
B/4	16	1111111111010010
B/5	16	1111111111010011
B/6	16	1111111111010100
B/7	16	1111111111010101
B/8	16	1111111111010110
B/9	16	1111111111010111
B/A	16	1111111111011000
C/1	10	1111111010
C/2	16	1111111111011001
C/3	16	1111111111011010
C/4	16	1111111111011011
C/5	16	1111111111011100
C/6	16	1111111111011101
C/7	16	1111111111011110
C/8	16	1111111111011111
C/9	16	1111111111100000
C/A	16	1111111111100001
D/1	11	11111111000
D/2	16	1111111111100010
D/3	16	1111111111100011
D/4	16	1111111111100100
D/5	16	1111111111100101
D/6	16	1111111111100110
D/7	16	1111111111100111
D/8	16	1111111111101000
D/9	16	1111111111101001
D/A	16	1111111111101010
E/1	16	1111111111101011
E/2	16	1111111111101100
E/3	16	1111111111101101
E/4	16	1111111111101110
E/5	16	1111111111101111
E/6	16	1111111111110000
E/7	16	1111111111110001
E/8	16	1111111111110010
E/9	16	1111111111110011
E/A	16	1111111111110100
F/0(ZRL)	11	11111111001
F/1	16	1111111111110101
F/2	16	1111111111110110
F/3	16	1111111111110111
F/4	16	1111111111111000
F/5	16	1111111111111001
F/6	16	1111111111111010
F/7	16	1111111111111011
F/8	16	1111111111111100
F/9	16	1111111111111101
F/A	16	1111111111111110

ハフマン符号化テーブル

【図１６】

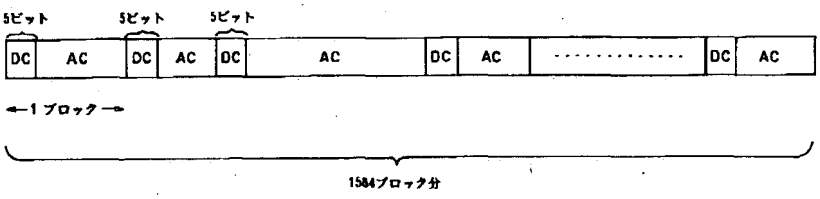
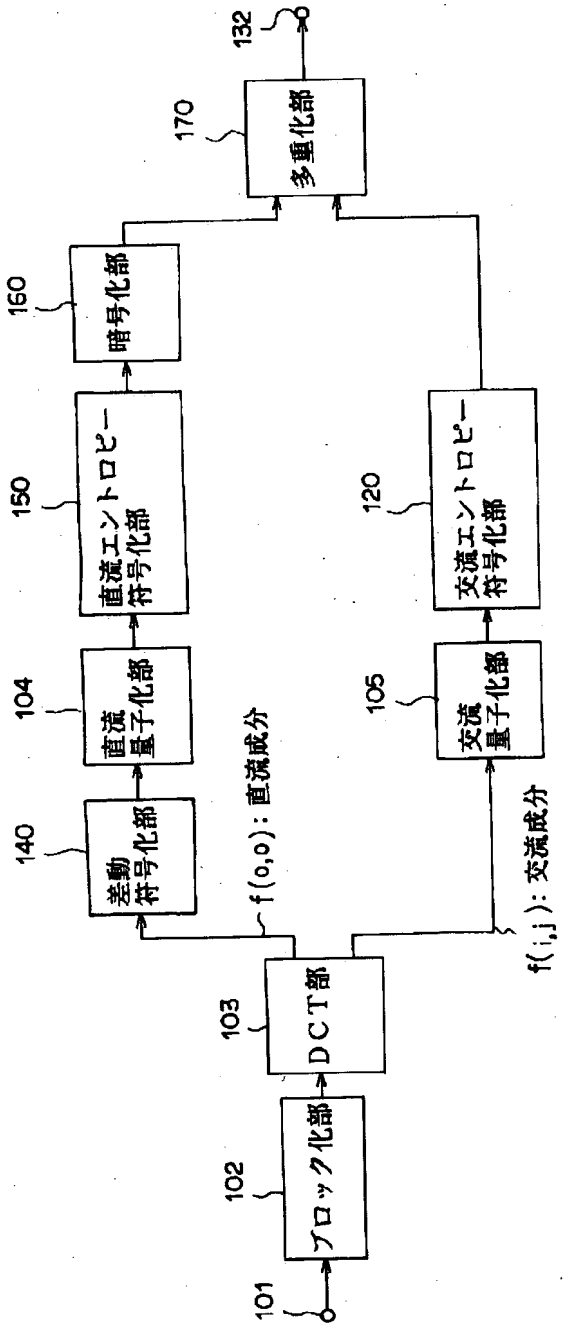


図１の多重化部の出力信号のフォーマット

【図１７】



本発明の第２の実施例の画像データ暗号化方法

【図１８】

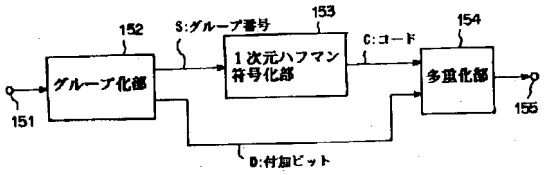


図１７の直流エントロピー符号化部

【図２０】

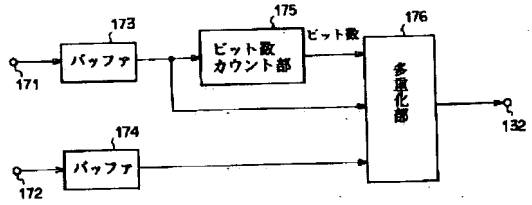


図１７の多重化部

【図２１】

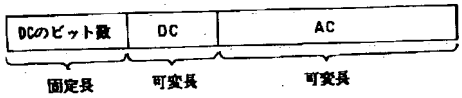


図１７の多重化部の出力信号のフォーマット

【図１９】

S	C
0	0 0
1	0 1 0
2	0 1 1
3	1 0 0
4	1 0 1
5	1 1 0
6	1 1 1 0
7	1 1 1 1 0
8	1 1 1 1 1 0
9	1 1 1 1 1 1 0
1 0	1 1 1 1 1 1 1 0
1 1	1 1 1 1 1 1 1 1 0

ハフマン符号化テーブル

フロントページの続き

(51)Int.Cl.5		識別記号	庁内整理番号	F I	技術表示箇所
H04L	9/14				
H04N	1/41		B 9070－5C		
	1/415		9070－5C		
	1/44		2109－5C		
	7/133		Z		